BCOP aneb jak správně nasazovat

Ondřej Caletka

6. června 2017

Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

Best Current Operational Practice Task Force

- nepříliš formální pracovní skupina v rámci RIPE komunity
- zaměřeno na konkrétní témata
- sdílení nejlepší současné praxe
- vysoké nároky na koncentrovanost a čtivost
  - rozsah kolem deseti stran
  - manažerské shrnutí na úvod
- zaměřeno na aktuální nejlepší současnou praxi, neřeší budoucnost

Best Current Operational Practice for operators: IPv6 prefix assignment for end-customers − persistent vs non-persistent, and what size to choose

DRAFT v.2 (published on 11th May 2017)

`https://sinog.si/docs/draft-IPv6pd-BCOP-v2.pdf`

Manažerské shrnutí

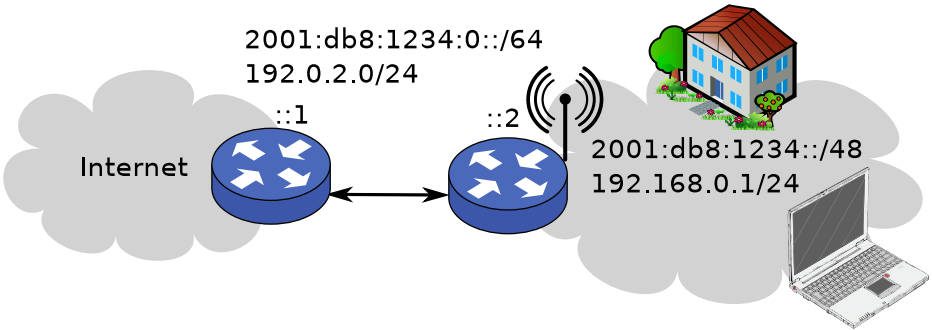
- IPv6 se liší od IPv4
- zejména v adresování zákazníků
- špatná rozhodnutí během plánování → zásadní potíže v provozu
  - například nutnost přeadresovat síť
- je třeba myslet ve velkém, není důvod šetřit
- časté změny adres jsou škodlivé

Cílová skupina

- operátoři (ISP), poskytující přístup k Internetu
  - rezidentním zákazníkům
  - malým a středním podnikům
- bohaté zkušenosti s IPv4
- minimální zkušenosti s IPv6
  - špatný adresní plán
  - nedomyšlení problematických míst

Přidělování prefixu koncovému uživateli

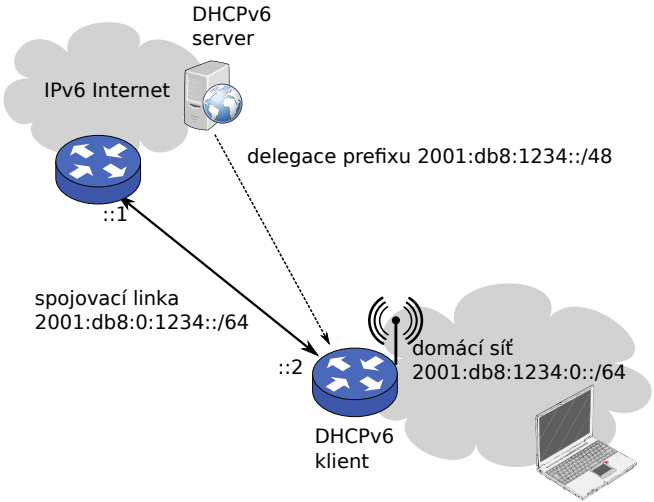
- nemá obdoby v IPv4
- musí vystačit pro všechny případné budoucí potřeby zákazníka
- přehnané šetření není na místě
  - při přidělování /48 trvale každému člověku vystačí 480 let
  - přílišné šetření způsobuje mnohem vážnější problémy



Adresování WAN linky

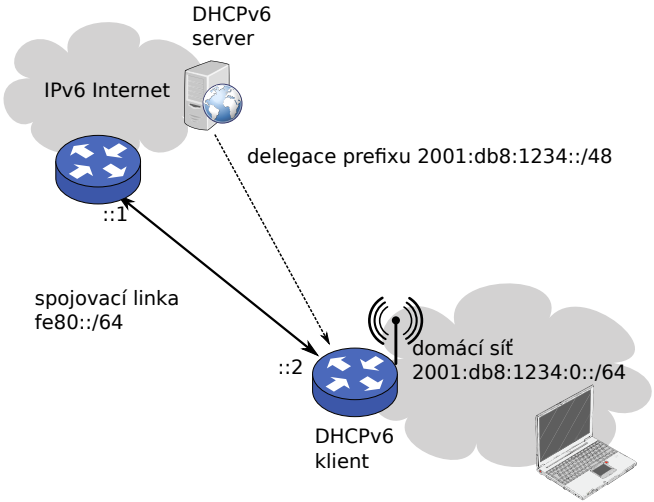
- /64 z vyhrazeného prefixu
- pouze Link-Local adresy
- unikátní lokální (ULA) adresy
- /64 z prefixu přiděleného zákazníkovi

/64 z vyhrazeného prefixu



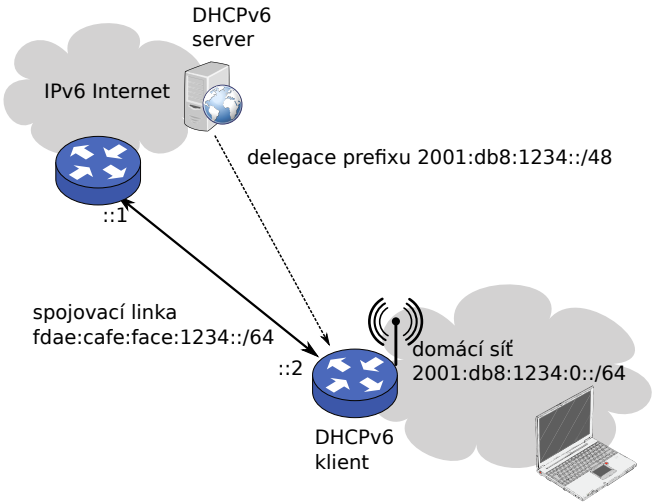
- nejčastější nasazení
- funguje s routery i koncovými stanicemi
- v závislosti na HW je možné použít delší prefix, až /127 pro PtP spoj
- je lepší v adresním plánu vyhradit /64

Pouze Link-Local adresy



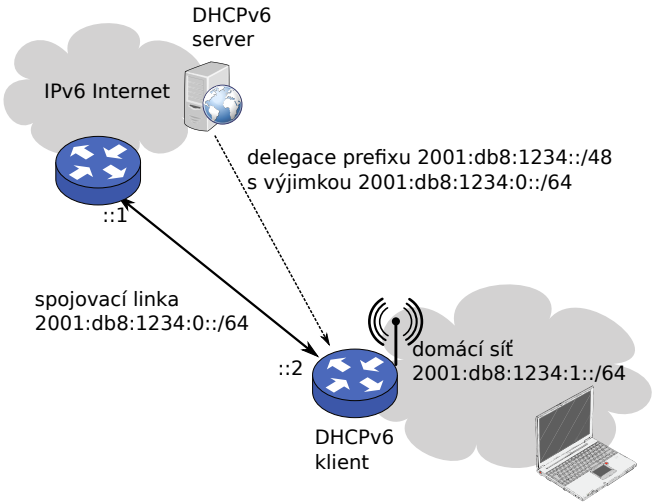
- problémy s kompatibilitou
- nefunguje s koncovými stanicemi
- obtížnější hledání potíží
- může ušetřit prostředky

Unikátní lokální adresy



- silně nedoporučováno
- obtížná komunikace CPE s okolním světem
  - například pro generování ICMP zpráv
  - rozbije objevování MTU cesty
- chybné implementace výběru zdrojové adresy

/64 z prefixu přiděleného zákazníkovi



- nejčistší z hlediska síťové topologie a směrování
- vyžaduje podporu RFC6603
- známé problémy se současnými CPE

Shrnutí adresování WAN linky

- /64 z vyhrazeného prefixu je všeobecně nejlepší přístup
- Link-Local nebo /64 ze zákaznického prefixu může fungovat za specifických podmínek
- ULA raději nepoužívat

Velikost přiděleného prefixu

- používání násobků 4 bitů je praktické
  - lze vyjádřit ve formátu např. `2001:db8:aaaa:cdXX::`
  - lze delegovat jako jednu reverzní DNS zónu
- pravidla regionálních registrů (např. RIPE NCC) dovolují přidělit až /48 na zákazníka
- minimální příděl /64 není dlouhodobě udržitelný a nedovoluje zákaznickou síť dále dělit
- naprosté minimum je několik /64

Prefix /48 pro všechny

- nejpraktičtější rozhodnutí
- dostatečný prostor i pro velké zákazníky
- kompatibilní s přechodovými mechanizmy (6to4)
- kompatibilní s unikátními lokálními adresami

Příklady obsazenosti

alokace	/48 celkem	/48 *zaplněno*[1]	/56 celkem	/56 *zaplněno*[1]
/32	65 536	24 155	16 777 216	6 183 533
/29	524 288	170 570	134 217 728	43 665 787

[1] prahová hodnota pro získání další alokace – H/D faktor 0.94

Prefix /56 pro domácí zákazníky

- především obchodní rozhodnutí
- dostatečný prostor pro malé a střední zákazníky
- stále umožní např. nasazení technologie Homenet

Tip

Při plánování vyhraďte pro každého zákazníka /48, ze kterého přidělte pouze /56. Pokud se v budoucnu plány změní, bude přechod bezbolestný.

Prefix delší než /56

- silně nedoporučovaná varianta
- není k tomu žádný důvod
- už /56 představuje rozumný kompromis
- přidělení pouze /64 je vyloženě škodlivé
  - nelze zřídit například ani síť pro hosty
  - nelze zapojit další router do kaskády
  - nebude fungovat protokol Homenet

Poznámka: Nelegální poskytovatelé internetu

- kdo poskytuje připojení zákazníkům, **musí mít adresy *alokované***
- typicky vstoupením do RIPE NCC a získáním /32 až /29
- z alokace lze *přidělovat* prefixy až /48 pro zákazníky
- jednou přidělené adresy není možné sdílet s dalšími
  - například přidělený prefix /48 dělit mezi zákazníky
- stejně tak je zakázáno přerozdělovat *Provider Independent* adresy (ty jsou v RIPE NCC z prefixu `2001:678::/29`)
- někteří *podnikavci* **zneužívají** neznalosti malých ISP a nabízí obstarání PI adres či pronájem *za výhodné ceny*

Stálost přiděleného prefixu

stálý prefix se nemění, bez ohledu na to, kolikrát uživatel připojí a odpojí zařízení nebo obnoví zápůjčku[1]

nestálý prefix se obvykle mění při každém navázání spojení

Podivná praxe některých ISP

- vynucený výpadek služby každých 24 hodin cca. na 20 sekund
- přidělení jiné IP adresy
- rozpad všech spojení

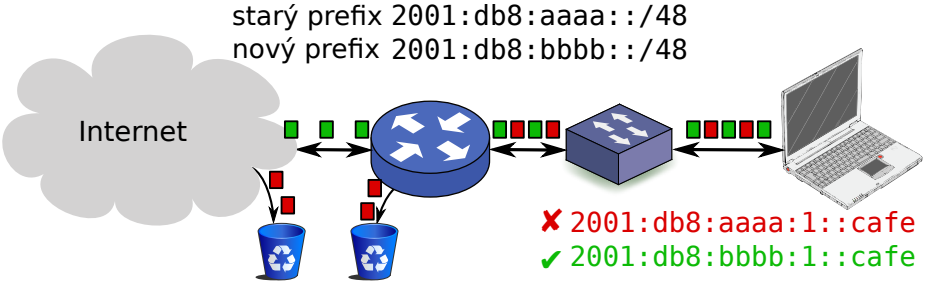
[1] může se ale změnit při přestěhování uživatele nebo rekonfiguraci sítě

Nestálé přidělování prefixu je snadné

- minimální požadavky na infrastrukturu
- dobrá agregovatelnost
- konzistentní s IPv4
- NAT skrývá problémy způsobené přeadresováním

Přeadresování v IPv6

- není přímá vazba mezi adresou a bránou
- brána musí aktivně anulovat starou adresu
- jinak bude koncové zařízení používat starou adresu nadále
- problém např. při ztrátě napájení CPE



Stálý je nejlepší

- vyžaduje složitější konfiguraci
- zjednodušuje evidenci, kdo má kterou adresu
- nutnost pro větší zákazníky
- možnost i např. delegovat reverzní DNS zónu
- nemusí být stálý *navždy*
  - může se změnit při změně technologie/stěhování
  - může se změnit při dlouhodobé neaktivitě (> týden)
  - ale neměl by se měnit při odpojení na několik hodin
- WAN linka může používat nestálý prefix, je-li to výhodné

Další vývoj BCOP

- pracovní skupina BCOP je otevřena námětům na podobné dokumenty z dalších oblastí nejlepší současné provozní praxe
- již hotový dokument MANRS: *Mutually Agreed Norms for Routing Security Implementation Guide*
- příprava obdobného dokumentu o IPv6 v prostředí hostingových a housingových center
- námět na BCOP dokument o správné implementaci DNS služeb (v reakci na aktivitu dns-violations)
- sledujte e-mailovou konferenci BCOP, máte-li zájem se podílet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz

Prezentace je již nyní k dispozici ke stažení.